

- 31 -

ABSTRACT

A terminal of a user as an issuer of electronic information calculates a Digest value for a content and sends this Digest value and a key ID of the issuer user to an authentication center server device. The authentication center server device searches a key storage for a secret key corresponding to this key ID, generates a signature value by encrypting the Digest value with this secret key and responds the signature value to the user terminal. The user terminal forms an undersigned content by attaching the received signature value and key ID to signature object electronic information, and issues this content to a recipient. The terminal of the recipient user calculates a Digest value for the content in the undersigned content, and sends this Digest value, the signature value and the attachment key ID to the authentication center server device. The authentication center server device searches the key storage for a public key corresponding to the key ID, decrypts the signature value with this public key, makes authentication as to whether a result of this decryption is coincident with the Digest value or not, and responds a result of the authentication to the user terminal.